

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 24 OCT 2014		2. REPORT TYPE N/A		3. DATES COVERED	
4. TITLE AND SUBTITLE Quality and Software Assurance				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Woody /Carol				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 1	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Quality and Software Assurance

Vulnerabilities are Defects

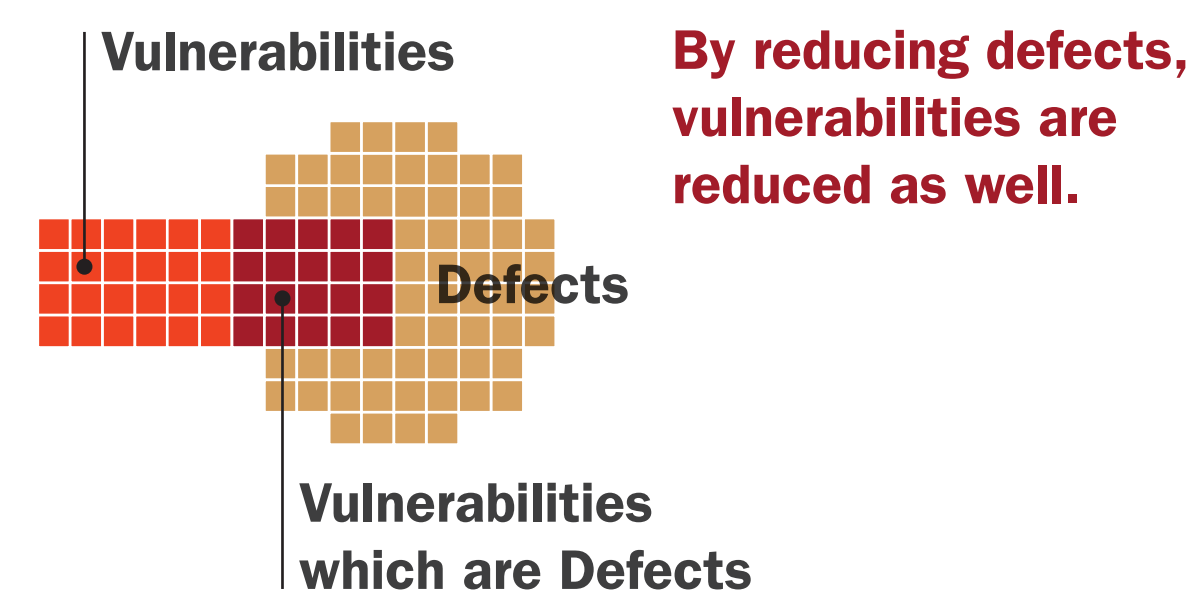
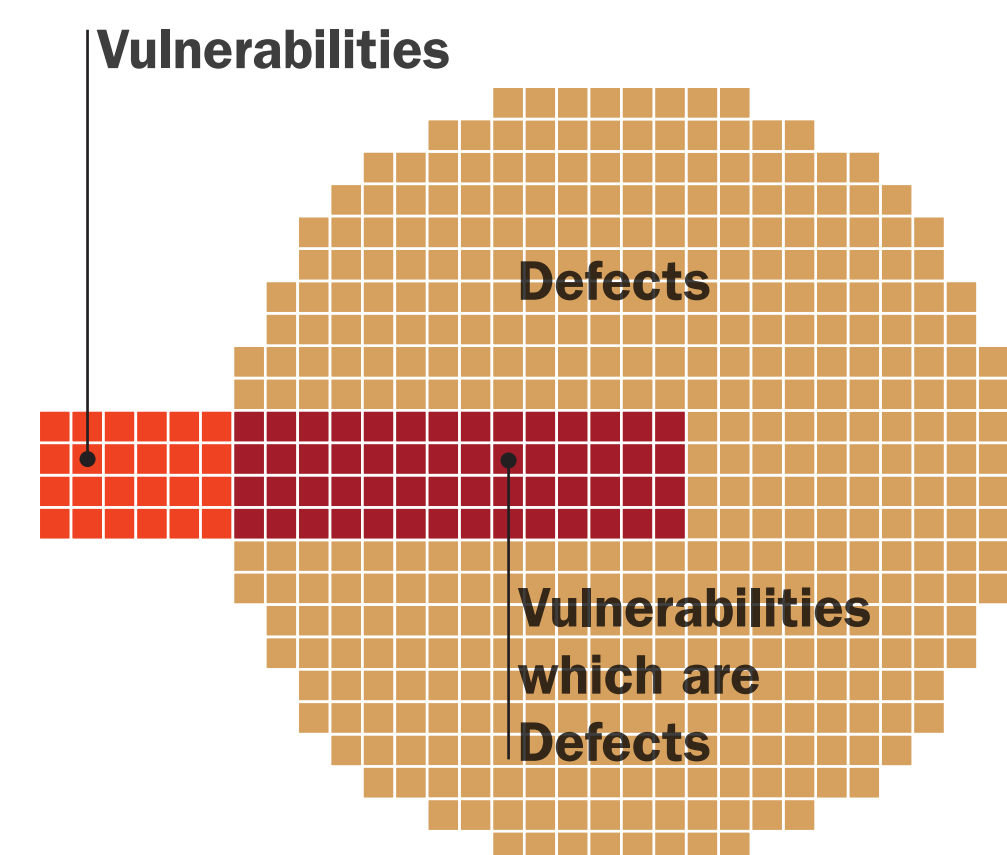
Literature Review: Vulnerabilities are 1-5% of defects Analysis of defects for five versions of Microsoft windows operating systems and two versions of Red Hat Linux systems) (Alhazmi, et.al., 2007)

Win 95 (14.5 MLOC) and Win 98 (18 MLOC) vulnerabilities are 1.00% and 0.84% respectively of identified defects

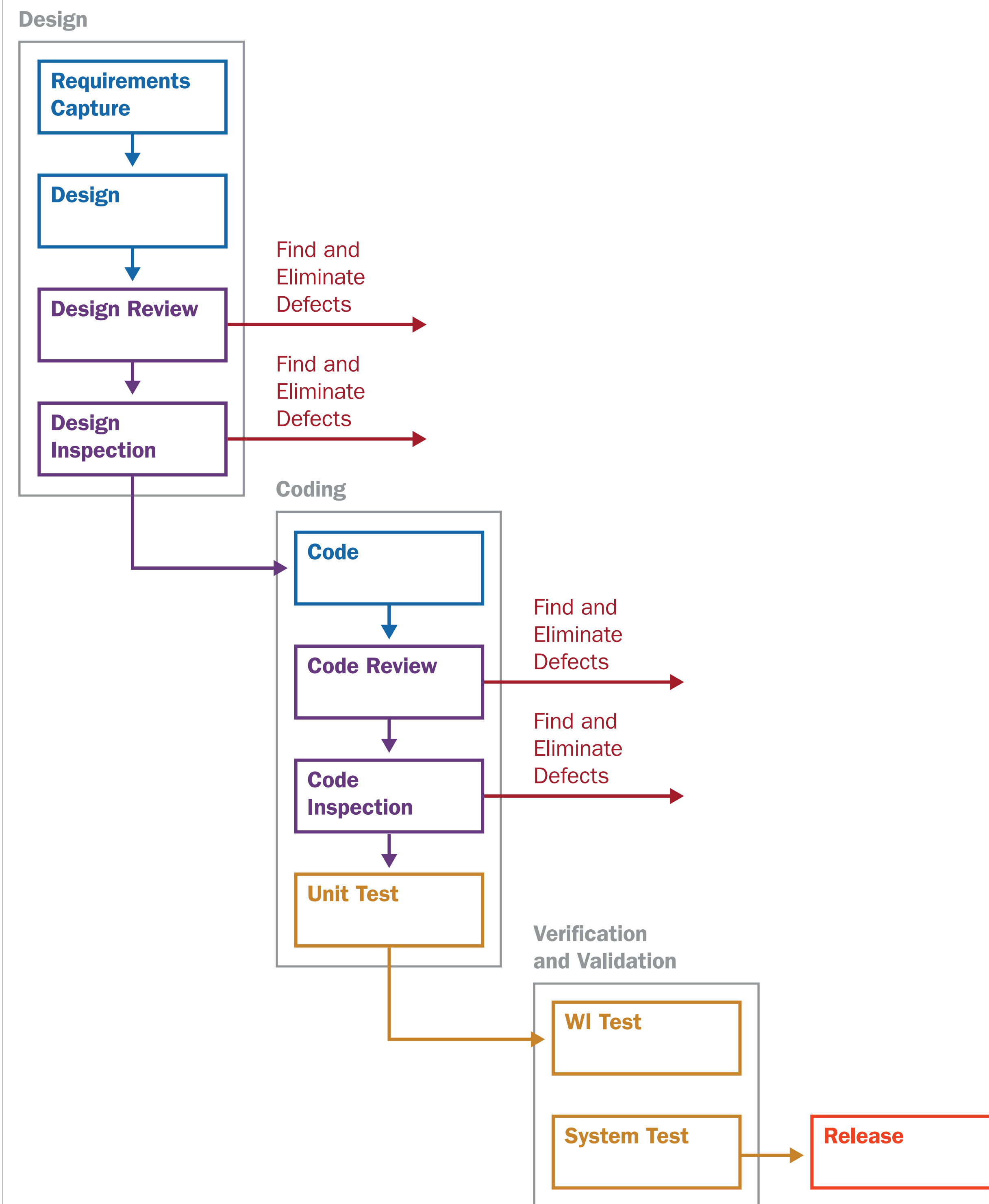
Red Hat Linux 6.2 (1.8 MLOC) and 7.1 (6.4 MLOC) vulnerabilities are 5.63% and 4.34% respectively of identified defects. Tom Longstaff asserted that vulnerabilities might represent 5% of total defects

(<http://research.microsoft.com/en-us/um/redmond/events/swsecinstitute/slides/longstaff.pdf>)

Ross Anderson: "it's reasonable to expect a 35,000,000 line program like Windows 2000 to have 1,000,000 bugs, only 1% of them are security-critical." (Anderson, 2001) Experiment: Evaluating an open source product to test predictions



Workflow for Quality and Software Assurance



Can Predictions of Quality Inform Security Risk Predictions?

The SEI has quality data for over 100 Team Software Process (TSP) development projects used to predict operational quality.

Data from five projects with low defect density in system testing reported very low or zero safety critical and security defects in production use.

HYPOTHESIS: A sufficiently low level of defects measured in test and production will reasonably predict very low risk of escaped safety critical or security vulnerabilities

